UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/937,397	04/01/2002	Jean-Sebastien Coron	032326-168	9400

21839 7590 04/18/2006

BUCHANAN INGERSOLL PC
(INCLUDING BURNS, DOANE, SWECKER & MATHIS)
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
PATEL, NIRAV B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 04/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/937,397	CORON, JEAN-SEBASTIEN	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2006 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date N/A.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on February 28, 2006 has been entered.

2. Claims 1-15 are pending.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-15 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-7 of U.S. Patent No. 6,914,986 (hereinafter '986 Patent).

As per claims 1, 6 and 11 of instant application, '986 Patent discloses similar a countermeasure method in an electronics component implementing a public

key cryptography algorithm based on the use of elliptical curves [col. 6 lines 21-23 "A countermeasure method in an electronic component using a public key cryptography algorithm based on the use of elliptic curves in which a private key d and the number of points n on an elliptic curve"].

drawing a random number k [col. 6 line 31 "taking a random value r"], calculating the integer d' = d + k*n [col. 6 line 32 "calculating an integer d' such that d'=d + r"],

calculating Q = d'* P [col. 6 lines 33-34 "Performing a scalar multiplication operation whose result is a point Q' on the curve such that Q'=d'.P"],

performing the scalar multiplication operation S = d.R [col. 6 lines 35-36 "Performing a scalar multiplication operation whose result is a point S on the curve such that S=r.P"],

calculating Q = Q' – S [col. 6 line 37 "calculating the point Q on the curve such that Q = Q'-S].

The limitation of claims 1, 6 and 11 cover the same subject matter as in '986 Patent except: *to determine a security parameter s.* It would have been obvious to a person of ordinary skill in the art at the time the invention was made to determine security parameter of the algorithm. The ordinary skilled person would have been motivated to improve the inherent security feature of the algorithm within the secure transaction application such as the use of the smartcard.

As per claims 2 and 7 of instant application, claim 2 of '986 Patent recites the same limitations.

As per claims 3, 8, 12 and 15 of instant application, claim 3 of '986 Patent recites the same limitations.

As per claims 4, 9 and 13 of instant application, claim 4 of '986 Patent recites the same limitations.

As per claims 5 and 10 of instant application, claims 5 and 6 of '986 Patent recites the same limitations.

As per claim 14 of instant application, claim 7 of '986 Patent recites the same limitations.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-15 are rejected under 35 USC 103 (a) for being unpatentable over Jerome A. Solinas ("An Improved Algorithm for Arithmetic on a Family of Elliptic Curves" 1998) and in view of Curiger et al (US Patent No. 6,064,740).

As per claims 1, 6 and 11 Solinas teaches:

public key cryptography algorithm based on the use of elliptical curve [page 357, lines 1-2], the operation Q = d*P [page 357 lines 3-5].

determining a security parameter s, drawing a random number k between 0 and 2^s

calculating the integer d' = d + k*n, calculating Q = d' * P [page 360 lines 6-7 "elliptic scalar multiplication", Algorithm 2, page 361 Algorithm 3 "Addition-Subtraction Method"].

elliptical curves defined on a finite field GF (p) [page 357 lines 1-2],

executing the scalar multiplication operation Q = d.P [page 357 lines 3-5],

performing the reduction operation modulo p of the coordinates of the point Q [page 357 lines 8-9]

Curiger teaches the limitation of claims 1, 6 and 11 as: the modular math calculation method and apparatus that is substantially immune from a power monitoring attack intended to determine a private key. Curiger discloses the microprocessor core 12 [Fig. 1], which is where the majority of calculations are performed and where the other circuitry in the module is controlled. Curiger further discloses the math coprocessor 36 [Fig. 1] running the 8 bit instructions [col. 6 lines 55-62].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use microprocessor core for calculating the calculation (i.e. algorithm) and to control the modules. The ordinary skilled person would have been motivated to reduce the risk of the power monitoring attack [Curiger, lines 51-54] and to allow the algorithm be performed with less execution time [Solinas, abst. lines 8-9].

As per claims 2 and 7 Curiger teaches that new deciphering integer is calculated at each new execution of the deciphering algorithm [col. 2 lines 59-60, col. 3 lines 58-60, col. 4 lines 7-9].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Curiger et al. into the teaching of Solinas to utilize microprocessor core 12, which is where the majority of calculations are performed and where the other circuitry in the module is controlled. The modification would be obvious because one of ordinary skill in the art would be motivated to reduce the risk of the power monitoring attack [Curiger, lines 51-54].

As per claims 3-5, 8-10, 12, 13 and 15 Curiger teaches the counter at each execution of deciphering algorithm [Fig. 1 component 30 (Prog. Counter, PC increment)].

As per claim 14, the rejection of claim 11 is incorporated and further Solinas teaches: replacing R with 2.R [page 360 algorithm 2].

Response to Argument

5. Applicant's arguments filed February 28, 2006 have been fully considered but they are not persuasive.

Applicant argues that:

"The Office Action has not established that the pending claims of the present application are obvious in view of the claims of the '986 patent".

Examiner maintains that:

As per claim 1 of instant application, '986 Patent discloses similar a countermeasure method in an electronics component implementing a public key cryptography algorithm based on the use of elliptical curves [col. 6 lines 21-23 "A countermeasure method in an electronic component using a public key cryptography algorithm based on the use of elliptic curves in which a private key d and the number of points n on an elliptic curve"].

drawing a random number k [col. 6 line 31 "taking a random value r"], calculating the integer d' = d + k*n [col. 6 line 32 "calculating an integer d' such that d'=d + r"],

calculating Q = d'* P [col. 6 lines 33-34 "Performing a scalar multiplication operation whose result is a point Q' on the curve such that Q'=d'.P"],

performing the scalar multiplication operation S = d.R [col. 6 lines 35-36 "Performing a scalar multiplication operation whose result is a point S on the curve such that S=r.P"],

calculating Q = Q' – S [col. 6 line 37 "calculating the point Q on the curve such that Q = Q'-S].

As per claims 6

Step 2 → step 1 of '986, Step 3 → step 2 of '986, Step 4 → step 3 of '986, Step 5 → steps 4 and 5 of '986.

As per claims 11

Step 1 → step 1 of '986, Step 2 → step 2 of '986, Step 3 → step 3 of '986, Step 4 → step 4 of '986, Step 5 → step 5 of '986

The limitation of claims 1 and 6 cover the same subject matter as in '986 Patent except: *to determine a security parameter s.* It would have been obvious to a person of ordinary skill in the art at the time the invention was made to determine security parameter of the algorithm. The ordinary skilled person would have been motivated to improve the inherent security feature of the algorithm within the secure transaction application such as the use of the smartcard.

See Double Patenting Rejection above.

Applicant argues that:

"The Solinas article does not disclose the features recited in the pending claims and office action has not established a prima facie case of obviousness upon which a proper rejection can be based".

Examiner maintains that:

Solinas teaches the Elliptic Scalar Multiplication (Q = d.P) as claimed in present invention [claims 1, 6, 11] (for example, see step 4 of claim 1) [page 360]. Further, Solinas teaches calculation of the nonadjacent form (NAF) of the coefficient in algorithm

2, which corresponds to the claimed step 1, 2, 3 of claim 1 [page 360, algorithm 2] and calculation of the elliptic scalar multiplication using the NAF in algorithm 3, which corresponds to the claimed step 4 of claim 1[page 361 algorithm 3]. Elliptic public key protocols are based on scalar multiplication, therefore Solinas teaches the field of cryptography [page 357, introduction - lines 5-6].

In response to applicant's argument, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with the applicant was concerned, in order to be relied upon as basis for rejection of the claimed invention. See *In re Ortiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Solinas's field of teaching is sufficient.

Curiger teaches the circuitry which performs modular mathematics calculations in the field of public key cryptography that is immune from the timing and power attack [col. 2 lines 47-54]. Curiger discloses the microprocessor core 12 [Fig. 1], which is where the majority of calculations are performed and where the other circuitry in the module is controlled. Curiger further discloses the math coprocessor 36 [Fig. 1] running the 8 bit instructions [col. 6 lines 55-62]. Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the microprocessor core disclosed by Curiger to calculate the algorithms (as disclosed by Solinas) and to control the modules. The ordinary skilled person would have been motivated to reduce the risk of the power monitoring attack [Curiger, lines 51-54] and to allow the algorithm be performed with less execution time [Solinas, abst. lines 8-9].

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

6. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

KAMBIZ ZAND
PRIMARY EXAMINER

NBP
4/10/06